

REMARKS

Prior to entry of the present amendment, claims 1-34 were pending in the present application. Claim 10 is cancelled above. Claims 1, 13, 21, 24, 28, 32 and 34 are amended above. New claims 35-47 are added above. No new matter is added by the new claims or claim amendments. Entry is respectfully requested.

With regard to the Priority section of the Office Action, the Applicants note that the present application is a continuation-in-part application of United States Patent Application Number 09/960,610, filed September 21, 2001.

The parent 09/960,610 application claims the benefit of:

1. United States Provisional Application Serial No. 60/234,657, filed September 22, 2000,
2. United States Provisional Application Serial No. 60/240,611, filed October 16, 2000,
3. United States Provisional Application Serial No. 60/242,949, filed October 24, 2000, and
4. United States Provisional Application Serial No. 60/244,704, filed October 31, 2000.

The present continuation-in-part application further claims the benefit of:

1. United States Provisional Application Serial No. 60/249,946, filed November 20, 2000,
2. United States Provisional Application Serial No. 60/260,705, filed January 10, 2001, and
3. United States Provisional Application Serial No. 60/285,300, filed April 20, 2001.

Claim 30 stands rejected under 35 U.S.C. 112, first paragraph, for reasons stated in the Office Action. The feature claimed in claim 30 is supported in the specification as filed at least at page 79, line 12 - page 81, line 4, and corresponding FIGs. 44-47. In particular, the feature of interleaving and encrypting each status message is supported in the specification at least at page 80, lines 7-8, 17-18, and 27-28. The concepts of interleaving and encrypting of data are enabled at least by the discussion in the specification as filed of FIGs. 3 and 4 at page 23, line 15-page 36, line 10. Reconsideration and removal of this rejection are respectfully requested.

Claims 1-7 and 24-29 stand rejected under 35 U.S.C. 102(e) as being anticipated by Mooney, *et al.* (U.S. Patent No. 6,351,813). Claims 21-23 and 32-34 stand rejected under 35 U.S.C. 102(b) as being anticipated by Hsu (U.S. Patent No. 5,754,647). Claims 8-20 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Mooney, *et al.* in view of Ciacelli, *et al.* (U.S. Patent No. 6,236,727). Claims 30 and 31 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Mooney, *et al.* Reconsideration and removal of the rejections are respectfully requested.

In the present invention as claimed in independent claim 1, a method for preventing unauthorized use of digital content data to be transferred from a first system to a second system includes “locating an archive of a digital content data at the first system”, and “determining transaction data of the second system that identifies the second system”. The method further includes “modifying the archive using the transaction data of the second system that identifies the second system to generate a modified archive” and “transferring the modified archive from the first system to the second system”.

Mooney, *et al.* discloses a method of preventing unauthorized transfer of digital content from a first system to a second system. In Mooney, *et al.*, a system 1110 converts unencrypted source files 1120 into encrypted files 1130 using a key 1140 generated by inputs from a user, User A, and a smart card 1150. The files are transmitted to a remote

site in their same encrypted form 1165 and decrypted by system 1170 using a key 1195, which is identical to key 1140. Key 1195 is created by, and obtained from, User A (see Mooney, *et al.*, FIG. 11 and column 6, lines 31-49). Mooney, *et al.* discloses requiring a user to enter a number of passwords in order to access a number of security levels. When a number of incorrect passwords have been entered, the security level to which access was attempted, and all lower security levels, are locked out to prevent further access by the user (see Mooney, *et al.*, column 5, lines 27-50). Upon proper entry of a number of passwords, a user can select a key for encryption of the data. The key can optionally be transferred to the recipient user, User B, via smart card 1190 to allow for data decryption at the user end.

It is submitted that Mooney, *et al.* fails to teach or suggest the method as claimed. In particular, Mooney, *et al.* fails to teach or suggest a method for preventing unauthorized use of digital content data that includes “modifying the archive using the transaction data of the second system that identifies the second system to generate a modified archive”. Instead, in Mooney, *et al.*, the key used to decrypt the data transferred from system 1110 was created by, and obtained from, User A, rather than being based on transaction data from the second system that identifies the second system, as claimed in claim 1. Since, Mooney, *et al.* fails to teach or suggest such a “modified archive”, it follows that Mooney, *et al.* further fails to teach or suggest “transferring the modified archive from the first system to the second system”. In Mooney *et al.*, no such “modified archive” exists, since the encrypted data that is passed is not based on the transaction data of the recipient system as claimed in claim 1. Accordingly, reconsideration of the rejection of independent claim 1 under 35 U.S.C. 102(e) as being anticipated by Mooney, *et al.*, and allowance of the claim, are respectfully requested.

The limitation of “modifying...second system” added to amended claim 1 is incorporated, in part, from former independent claim 10. Claim 10 stands rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of Mooney, *et al.* and

Ciacelli, *et al.* (U.S. Patent No. 6,236,727).

With regard to the rejection of former claim 10 in view of the combination of Ciacelli, *et al.* and Mooney, *et al.*, Ciacelli, *et al.* discloses a method for protecting copyright data within a computer system. With reference to FIG. 1 of Ciacelli, *et al.* it is determined at a primary software module 22 whether data needs to be protected during subsequent transmission from the CPU. If such protection is desired, the primary module 22 advises the designated system that is to receive the stream of data, such as secondary module 20 and/or device 30, to download a suitable decryption algorithm. An encryption key is generated at the primary module 22 which is used to encrypt the original data, and the encrypted key and the encrypted data are combined into a data stream, which is then transmitted through memory 25 to the recipient system 20, 30 (see Ciacelli, column 3, lines 55-66 and column 6, lines 3-53).

Like Mooney, *et al.*, Ciacelli, *et al.* fails to teach or suggest a method for preventing unauthorized use of digital content data that includes “modifying the archive using the transaction data of the second system that identifies the second system to generate a modified archive” and “transferring the modified archive from the first system to the second system”, as claimed in claim 1. Instead, in Ciacelli, *et al.*, an encryption/decryption algorithm pair and associated key are determined at a primary module 20 and sent to a receiving system. Ciacelli, *et al.* in no way teaches “modifying the archive using the transaction data of the second system that identifies the second system”, as claimed in claim 1. In Ciacelli, *et al.*, modification of the data is not based on the transaction data of the recipient system. Since Ciacelli, *et al.* fails to teach or suggest such a “modified archive”, Ciacelli, *et al.* further fails to teach or suggest “transferring the modified archive from the first system to the second system”, as claimed in claim 1.

Since neither Mooney, *et al.* nor Ciacelli, *et al.* teach or suggest this limitation, there is no combination of the references that would teach or suggest this limitation.

Accordingly, reconsideration and removal of the rejection of former claim 10 as may be applied to amended independent claim 1, and allowance of claim 1, are respectfully requested.

With regard to the rejection of dependent claims 2-7 under 35 U.S.C. 102(e) as being anticipated by Mooney, *et al.* and new claims 35, 36, and 38-42, it is submitted that these claims should inherit the allowability of the independent claim from which they depend. Such allowance is respectfully requested.

With regard to the rejection of claims 8-9, and 11-20 under 35 U.S.C. 103(a) as being unpatentable over the combination of Mooney, *et al.* and Ciacelli, *et al.* and new dependent claim 37, it is submitted that the combination of Mooney, *et al.* and Ciacelli, *et al.* fails to teach or suggest a method for preventing unauthorized use of digital content data includes “modifying the archive using the transaction data of the second system that identifies the second system to generate a modified archive” and “transferring the modified archive from the first system to the second system”, as claimed in independent claim 1, as described above, from which claims 8-9 and 11-20 and new dependent claim 37 depend. Accordingly, reconsideration and removal of the rejection of claims 8-9 and 11-20, and allowance of the claims are respectfully requested.

In the present invention as claimed in independent claim 24, a method for preventing unauthorized use of digital content data hosted on a system includes, determining whether an unauthorized use of digital content data is in progress, and “in the case where an unauthorized use is determined, initiating a defense action by disabling only an input device in association with the unauthorized use”.

With regard to the rejection of independent claim 24, Mooney, *et al.* fails to teach or suggest a method for preventing unauthorized use of digital content data hosted on a system including, “in the case where an unauthorized use is determined, initiating a

defense action by disabling only an input device in association with the unauthorized use”, as claimed in claim 24. Instead, Mooney, *et al.*, discloses that the security level at which access is improperly attempted, and all lower security levels, are locked out when a number of incorrect passwords are entered, thus, the entire system is locked out.. There is no mention in Mooney, *et al.* of disabling only an input device in association with the unauthorized use, as claimed in claim 24. Accordingly, reconsideration of the rejection of independent claim 24 under 35 U.S.C. 102(e) as being anticipated by Mooney, *et al.*, and allowance of the claim, are respectfully requested. With regard to the rejection of dependent claims 25-27 and new dependent claims 44 and 45, it follows that these claims should inherit the allowability of independent claim 24, from which they depend.

In the present invention as claimed in independent claim 28, a method for preventing unauthorized use of digital content data hosted on a system includes “executing a plurality of system processes”, “monitoring at each process for unauthorized use and each process transferring a status message to another process related to the unauthorized use”, and “each process determining whether unauthorized use has occurred, and, if such a determination is made, initiating a nondeterministic defense action wherein the nondeterministic defense action obfuscates the cause of the defense action”.

With regard to the rejection of claim 28, Mooney, *et al.* in no way teaches or suggests “monitoring at each process for unauthorized use and each process transferring a status message to another process related to the unauthorized use”, as claimed in claim 28. Further, Mooney, *et al.* fails to teach or suggest “each process determining whether unauthorized use has occurred, and, if such a determination is made, initiating a nondeterministic defense action wherein the nondeterministic defense action obfuscates the cause of the defense action”, as claimed in claim 28. Instead, in Mooney, *et al.*, entry of an incorrect password causes the system to be locked out. This is a deterministic action, in the sense that the lockout is a repeatable action that would be obvious to an

observer, the lock out being initiated in response to entry of incorrect passwords by an unauthorized user. Mooney, *et al.* therefore does not obfuscate the cause of the defense action as claimed in claim 28 of the present invention. Accordingly, reconsideration of the rejection of independent claim 28 under 35 U.S.C. 102(e) as being anticipated by Mooney, *et al.*, and allowance of the claim, are respectfully requested.

With regard to the rejection of dependent claim 29 under 35 U.S.C. 102(e) as being anticipated by Mooney, *et al.* and new dependent claim 46, it is submitted that these claims should inherit the allowability of the independent claim from which they depend. Such allowance is respectfully requested. With regard to the rejection of dependent claims 30 and 31 under 35 U.S.C. 103(a) as being unpatentable over Mooney, *et al.*, it is submitted that these claims should inherit the allowability of the independent claim from which they depend. Such allowance is respectfully requested.

In the present invention as claimed in independent claim 21, a method for preventing unauthorized use of digital content data hosted on a system includes "initiating a nondeterministic defense action if it is determined that an emulator device is operating on the system, wherein the nondeterministic defense action obfuscates the cause of the defense action".

Hsu discloses a method of software protection utilizing read-write memory means. The emulator detector 60 utilizes a mode control select signal SEL to control the operation of an inconsistent read-write memory 32, so that erroneous data is read out continuously or intermittently when an emulator program memory "dumping" attempt is detected. The mode control select signal controls the erroneous data in each instance. In another approach, the emulator detector 60 continuously or intermittently applies a power supply voltage or a ground voltage to the signal lines in the address bus 20, data bus 22, and control bus 24, so that erroneous data is read out continuously or intermittently when an emulator program memory "dumping" attempt is detected. Thus, the same action of

pulling the bus signal lines up to the power supply or down to the ground potential occurs each time a data dump is detected.

Hsu fails to teach or suggest “initiating a nondeterministic defense action if it is determined that an emulator device is operating on the system, wherein the nondeterministic defense action obfuscates the cause of the defense action”, as claimed in claim 21. Instead, in Hsu, in both methods, when a memory dump operation is detected, erroneous data is provided, thus the Hsu response defensive action is the same each time and is therefore deterministic. The Hsu approach is deterministic in the sense that each time a memory dump is detected in Hsu, the same result occurs, namely the generation of erroneous data on a given bus. Hsu therefore does not obfuscate the cause of the defense action. Accordingly, reconsideration of the rejection of independent claim 21 under 35 U.S.C. 102(b) as being anticipated by Hsu and allowance of the claim, are respectfully requested. With regard to the rejection of dependent claims 22-23 and new dependent claim 43, it follows that these claims should inherit the allowability of independent claim 21, from which they depend.

In the present invention as claimed in independent claim 32, a method for preventing unauthorized use of digital content data hosted on a system includes “in the case where an unauthorized use is determined, initiating a nondeterministic defense action that is integrated into the function, wherein the nondeterministic defense action obfuscates the cause of the defense action”.

Hsu in no way teaches a method for preventing unauthorized use of digital content data hosted on a system that includes “in the case where an unauthorized use is determined, initiating a nondeterministic defense action that is integrated into the function” as claimed in claim 32, for the reasons described above. Further, Hsu, as discussed above, fails to teach or suggest “the nondeterministic defense obfuscates the cause of the defense action”, as claimed in claim 32. Accordingly, reconsideration of the


rejection of independent claim 32 under 35 U.S.C. 102(b) as being anticipated by Hsu and allowance of the claim, are respectfully requested. With regard to the rejection of dependent claims 33 and 34 and new dependent claim 47, it follows that these claims should inherit the allowability of independent claim 32, from which they depend.

Closing Remarks

It is submitted that all claims are in condition for allowance, and such allowance is respectfully requested. If prosecution of the application can be expedited by a telephone conference, the Examiner is invited to call the undersigned at the number given below.

Respectfully submitted,

Date: September 30, 2005
Mills & Onello, LLP
Eleven Beacon Street, Suite 605
Boston, MA 02108
Telephone: (617) 994-4900, Ext. 4902
Facsimile: (617) 742-7774
J:\ECD\0003\amenda\amendment2.wpd



Anthony P. Onello, Jr.
Registration Number 38,572
Attorney for Applicant